

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently Amended) A method for using query signatures to detect
2 structured query language (SQL) injection, comprising:
3 initializing a signature cache, wherein initializing the signature cache
4 involves:
5 trapping database queries in a controlled environment,
6 parsing the database queries to produce a set of valid signatures,
7 wherein parsing the database queries involves retaining SQL keywords
8 contained in each query, and removing field names and corresponding
9 values in each query, to determine the signature for each query;
10 wherein the signature for a query contains the text of SQL
11 keywords and operands without any field name or
12 value in the query, ~~determining signatures for the queries, wherein~~
13 ~~the signature SQL keywords contained in the corresponding query with~~
14 ~~literals removed, and~~
15 storing the valid signatures in the signature cache;
16 receiving a query at the database;
17 parsing the query at the database to determine a signature for the query,
18 wherein the signature comprises SQL keywords contained in the corresponding
19 query with literals removed;
20 determining if the signature is located in the signature cache, which
21 contains signatures for valid queries; and

22 if so, allowing the corresponding SQL query to proceed, processing the
23 query, otherwise, triggering a mismatch alert, identifying the query as being SQL
24 injected and rejecting the query.

1 2. (Cancelled)

1 3. (Previously presented) The method of claim 1, wherein the mismatch
2 alert throws an error.

1 4. (Previously presented) The method of claim 1, wherein the mismatch
2 alert is sent to a database administrator and the query is processed.

1 5. (Previously presented) The method of claim 1, wherein the mismatch
2 alert is sent to a requesting application, thereby allowing the requesting
3 application to take action.

1 6. (Cancelled)

1 7. (Original) The method of claim 1, wherein if the signature generates a
2 mismatch alert and if the query is a valid query, the method further comprises
3 allowing a database administrator to add the signature to the signature cache.

1 8. (Currently Amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method for using query signatures to detect SQL injection, wherein the computer-
4 readable storage medium includes magnetic and optical storage devices, disk
5 drives, magnetic tape, CDs (compact discs), and DVDs (digital versatile discs or
6 digital video discs), the method comprising:

7 initializing a signature cache, wherein initializing the signature cache
8 involves:
9 trapping database queries in a controlled environment,
10 parsing the database queries to produce a set of valid signatures,
11 wherein parsing the database queries involves determining retaining SQL
12 keywords contained in each query, and removing field names and
13 corresponding values in each query, to determine the signature for each
14 query;
15 wherein the signature for a query contains the text of SQL
16 keywords and operands without any field name or
17 value in the query, signatures for the queries, wherein the signature
18 comprises SQL keywords contained in the corresponding query
19 with literals removed, and
20 storing the valid signatures in the signature cache;
21 receiving a query at the database;
22 parsing the query at the database to determine a signature for the query,
23 wherein the signature comprises SQL keywords contained in the corresponding
24 query with literals removed;
25 determining if the signature is located in the signature cache, which
26 contains signatures for valid queries; and
27 if so, allowing the corresponding SQL query to proceed, processing the
28 query, otherwise, triggering a mismatch alert requesting further actions.
29 identifying the query as being SQL injected and rejecting the query.

1 9. (Cancelled)

1 10. (Previously presented) The computer-readable storage medium of
2 claim 8, wherein the mismatch alert throws an error.

1 11. (Previously presented) The computer-readable storage medium of
2 claim 8, wherein the mismatch alert is sent to a database administrator and the
3 query is processed.

1 12. (Previously presented) The computer-readable storage medium of
2 claim 8, wherein the mismatch alert is sent to a requesting application, thereby
3 allowing the requesting application to take action.

1 13. (Cancelled)

1 14. (Original) The computer-readable storage medium of claim 8, wherein
2 if the signature generates a mismatch alert and if the query is a valid query, the
3 method further comprises allowing a database administrator to add the signature
4 to the signature cache.

1 15. (Currently Amended) An apparatus for using query signatures to detect
2 SQL injection, comprising:
3 an initialization mechanism configured to initialize a signature cache,
4 wherein when initializing the signature cache, the mechanism is configured to:
5 trap database queries in a controlled environment,
6 parse the database queries to produce a set of valid signatures,
7 wherein parsing the database queries involves retaining SQL keywords
8 contained in each query, and removing field names and corresponding
9 values in each query, to determine the signature for each query;
10 wherein the signature for a query contains the text of SQL
11 keywords and operands without any field name or value in the
12 query, determining signatures for the queries, wherein the signature

13 comprises SQL keywords contained in the corresponding query with
14 literals removed, and
15 store the valid signatures in the signature cache;
16 a receiving mechanism configured to receive a query at the database;
17 a parsing mechanism configured to parse the query at the database to
18 determine a signature for the query, wherein the signature comprises SQL
19 keywords contained in the corresponding query with literals removed;
20 a matching mechanism configured to determine if the signature is located
21 in the signature cache, which contains signatures for valid queries;
22 a processing mechanism configured to process the query if the signature is
23 located in the signature cache; and
24 an alerting mechanism configured to trigger a mismatch alert ~~identify the~~
25 ~~query as being SQL injected and rejecting the query~~ if the signature is not located
26 in the signature cache.

1 16. (Cancelled)

1 17. (Previously presented) The apparatus of claim 15, wherein the
2 mismatch alert throws an error.

1 18. (Previously presented) The apparatus of claim 15, wherein the
2 mismatch alert is sent to a database administrator and the query is processed.

1 19. (Previously Presented) The apparatus of claim 15, wherein the
2 mismatch alert is sent to a requesting application, thereby allowing the requesting
3 application to take action.

1 20. (Cancelled)

1 21. (Original) The apparatus of claim 15, further comprising an adding
2 mechanism configured to allow a database administrator to add the signature to
3 the signature cache if the signature generates a mismatch alert and if the query is a
4 valid query.